



PRESIDÊNCIA DO CONSELHO DE MINISTROS
GABINETE NACIONAL DE SEGURANÇA

Comunicação 01/2021

Assunto: Utilização de assinaturas e selos eletrónicos qualificados em faturas eletrónicas.

Este comunicado enquadra-se nos termos de utilização dos serviços de confiança, previstos no Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança (Regulamento eIDAS).

Compete ao Gabinete Nacional de Segurança (GNS), enquanto entidade supervisora nacional, cujas competências constam do artigo 17.º do citado Regulamento e do artigo 12.º do Decreto-Lei n.º 28/2019, de 15 de fevereiro, para além de efetuar todas as esclarecimentos relativos aos **documentos eletrónicos em geral**, e às faturas eletrónicas de forma específica, ser o garante, por parte de todos os intervenientes, da observação constante do disposto nos artigos 25.º e 35.º do Regulamento eIDAS, relativos aos efeitos legais das assinaturas e selos eletrónicos.

Sendo os Prestadores Qualificados de Serviços de Confiança (PQSC), o foco principal desta comunicação, releva-se a importância, dadas as interligações existentes nesta matéria, que o conteúdo da mesma seja também transmitido a todos os restantes intervenientes, designadamente:

- Os operadores económicos;
- As empresas produtoras de software de faturação; e
- As plataformas de faturação eletrónica.

Atendendo à especificidade dos diversos pedidos de esclarecimento que nos têm chegado, e que abaixo se sintetiza em cinco respostas a outras tantas questões, pretende-se, desta forma, cobrir o maior leque possível de questões suscitadas.

A presente comunicação não versa sobre o enquadramento fiscal aplicável à faturação eletrónica ou outra forma de faturação.



PRESIDÊNCIA DO CONSELHO DE MINISTROS
GABINETE NACIONAL DE SEGURANÇA

Comunicação 01/2021

1. **É possível uma pessoa/entidade assinar/selar faturas eletrónicas de um terceiro, ao qual essa pessoa/entidade não está vinculada?**

A resposta é que NÃO é possível.

A resposta decorre do facto de que a assinatura eletrónica é o resultado de um processo eletrónico de dados suscetível de constituir objeto de direito individual e exclusivo de ser utilizado para dar a conhecer a autoria de um documento eletrónico, conforme definição constante no artigo 2.º do Decreto-Lei n.º 290-D/99, de 2 de agosto.

Para além disso, de acordo com o referido Decreto-Lei, a aposição de uma assinatura eletrónica qualificada a um documento eletrónico equivale à assinatura manuscrita dos documentos com forma escrita sobre suporte de papel e cria a presunção de que:

- A pessoa que após a assinatura eletrónica qualificada é o titular desta ou é representante, com poderes bastantes, da pessoa coletiva titular da assinatura eletrónica qualificada;
- A assinatura eletrónica qualificada foi aposta com a intenção de assinar o documento eletrónico;

Dado o exposto e considerando a natureza intransmissível de um certificado qualificado, assim como a sua associação inequívoca à identidade da pessoa (coletiva ou singular), entende-se que **NÃO SE PODE** utilizar um certificado qualificado para assinar documentos da autoria de terceiros.

O mesmo se aplica aos selos eletrónicos, nos termos previstos no artigo 35.º do Regulamento eIDAS.

Os PQSC devem, de forma pedagógica, alertar os seus potenciais clientes (titulares de certificados) para esta realidade.



Comunicação 01/2021

2. A assinatura/selagem de faturas, apenas é possível com recurso a certificados qualificados de selos eletrónicos ou certificados qualificados de assinatura com poderes de representação?

A resposta é que NÃO.

Embora não seja possível uma pessoa/entidade assinar/selar faturas eletrónicas de um terceiro, ao qual essa pessoa/entidade não está vinculada (vide pergunta 1), podem ser utilizados certificados qualificados de assinatura eletrónica individuais para assinar faturas eletrónicas, uma vez que não existe qualquer disposição legal que iniba a utilização deste tipo de certificados qualificados.

No entanto, o titular deste tipo de certificados, poderá ter de fornecer informação adicional aos destinatários da fatura, de modo a poder provar o vínculo existente entre o titular do certificado com a entidade emitente das faturas.

É ainda fundamental salientar que, entre os vários serviços de confiança previstos no Regulamento eIDAS, aquele que por excelência está vocacionado para ser utilizado por pessoas coletivas e consequentemente, para assinar faturas eletrónicas, é o “selo eletrónico”.

Os certificados qualificados de selo eletrónico já contem todos os dados indispensáveis à correta identificação da pessoa coletiva, o que, consequentemente, proporciona uma validação inquestionável entre os dados que constam no documento de faturação e os dados do selo eletrónico.

A identificação referida anteriormente, também é válida para os certificados de assinaturas com poderes de representação.

Os PQSC devem de forma pedagógica, alertar os seus potenciais clientes (titulares de certificados) para esta realidade, e recomendar para a assinatura/selagem da fatura eletrónica das entidades, a utilização de:

- Certificado qualificado de selo eletrónico da entidade;
- Certificado qualificado de assinatura eletrónica que inclua os poderes de representação do titular, em relação à entidade; ou
- Certificado qualificado de assinatura eletrónica, com a ressalva que nestes casos poderá ter de adicionar a prova da ligação entre o titular do certificado e a entidade emitente das faturas.



Comunicação 01/2021

3. Para assinar/selar faturas eletrónicas é possível usar certificados qualificados, nos quais as chaves estão guardadas em ficheiros com o formato “.pfx” ou “.p12”?

A resposta é que NÃO.

O Decreto-Lei n.º 28/2019, de 15 de fevereiro, que procede à regulamentação das obrigações relativas ao processamento de faturas e outros documentos fiscalmente relevantes, vem referir no seu artigo 12.º, relativo à emissão de faturas por via eletrónica que, para que seja garantida a autenticidade da origem e a integridade do conteúdo dos documentos, devem, entre outros, ser seguidos um dos seguintes procedimentos:

- Aposição de uma assinatura eletrónica qualificada nos termos legais;
- Aposição de um selo eletrónico qualificado, nos termos do Regulamento (UE) n.º 910/2014, do Parlamento Europeu e do Conselho, de 23 de julho de 2014;

O Regulamento eIDAS requer que as assinaturas/selos eletrónicos qualificados sejam criadas num dispositivo qualificado de criação de assinaturas/selos eletrónicos, pelo que a aposição de assinaturas/selos eletrónicos, que não cumpra esta exigência, não são consideradas adequadas para serem utilizadas nos termos previstos nas alíneas a) e b) do n.º 2 do artigo 12.º do Decreto-Lei n.º 28/2019, de 15 de fevereiro.

Os PQSC devem, de forma pedagógica, informar os seus potenciais clientes (titulares de certificados) para esta realidade, e recomendar para a assinatura/selagem da fatura eletrónica da entidade, a utilização de diversos tipos de dispositivos qualificados de criação de assinaturas/selos, consoante as necessidades desse cliente. Regra geral, as soluções disponibilizadas pelo PQSC, incluem dispositivos qualificados com as seguintes características:

- Smartcard ou Token USB: para titulares com baixo volume de assinaturas/selos;
- HSM¹ dedicados (on-premises): para titulares com grande volume de assinaturas/selos;
- Dispositivos qualificados geridos pelo PQSC: para todos o tipo de utilizadores, que optem por utilizar assinaturas remotas independentemente do volume.

¹ Hardware Security Module



PRESIDÊNCIA DO CONSELHO DE MINISTROS
GABINETE NACIONAL DE SEGURANÇA

Comunicação 01/2021

-
4. **É possível outras entidades, que não os PQSC, gerirem os dados de criação de assinatura de múltiplos titulares de certificados qualificados para a realização de assinaturas eletrónicas à distância?** Designadamente, outros fornecedores tecnológicos (plataformas de faturação, empresas gestoras de SW de faturação, etc.), podem operar e gerir as diversas chaves privadas (dados de criação de assinatura) dos seus clientes para assinatura à distância.
-

A resposta é que NÃO é possível.

O Regulamento eIDAS prevê a criação de assinaturas eletrónicas à distância. No entanto, de modo a garantir que estas assinaturas eletrónicas beneficiam do mesmo reconhecimento jurídico que as assinaturas eletrónicas criadas num ambiente inteiramente gerido pelo utilizador, os prestadores de serviços de assinatura à distância tem que aplicar procedimentos de segurança, de gestão e de administração específicos, utilizando sistemas e produtos fiáveis, de modo a garantir a fiabilidade do ambiente de criação de assinaturas eletrónicas e garantir que esse mesmo ambiente é utilizado sob a supervisão exclusiva do signatário.

Às assinaturas eletrónicas qualificadas criadas através de dispositivos de criação das assinaturas eletrónicas à distância, aplicam-se os requisitos previstos para PQSC, estabelecidos no citado Regulamento.

Salienta-se que os sistemas que permitem a realização e assinaturas eletrónicas à distância são sistemas complexos, sujeitos a requisitos de segurança muitos exigentes, nos quais é exigido que as chaves dos titulares sejam geradas e guardadas em módulos de hardware seguro, sujeitos a certificação autónoma.

O mesmo se aplica aos selos eletrónicos, nos termos previstos no artigo 35.º do Regulamento eIDAS.

Tais exigências têm como fundamento a necessidade de garantir que um atacante terá extremas dificuldades em descobrir ou derivar o valor das chaves para assinatura, de modo a que estas possam ser apenas usadas pelos legítimos titulares.

Em conclusão, apenas os PQSC, que constem nas listas de confiança de cada Estado-Membro, que disponibilizam serviços de confiança com o *qualifier* “*QCQSCDManagedOnBehalf*”², estão habilitados para tal. Os PQSC devem, de forma pedagógica, alertar os seus potenciais clientes (titulares de certificados) para esta realidade.

As listas de confiança de Estado-Membro, que inclui os prestadores e serviço qualificados, pode ser consultada em: <https://webgate.ec.europa.eu/tl-browser/#/>

² <https://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCQSCDManagedOnBehalf/>



PRESIDÊNCIA DO CONSELHO DE MINISTROS
GABINETE NACIONAL DE SEGURANÇA

Comunicação 01/2021

5. Nos sistemas de assinaturas à distância, o titular necessita de introduzir novas credenciais de autenticação, sempre que é aposta uma assinatura/selo numa fatura eletrónica?

A resposta é que NÃO.

As normas que suportam a implementação dos serviços de confiança descritos no Regulamento eIDAS, de modo a garantir um equilíbrio entre a operacionalidade das soluções e o controlo na utilização das assinaturas/selos à distância, permitem que sejam definidos critérios para limitar a reutilização de credenciais para acesso aos sistemas, designadamente, podem ser definidos por limite de “tempo” e/ou por limite de “quantidade”.

Essa reutilização de credenciais aplica-se apenas para efeitos de autenticação do titular perante o sistema, ou seja, apenas se cinge aos dados de autenticação e não aos dados de ativação das assinaturas (SAD³), tendo em consideração o estabelecido na norma EN 419241-1⁴, designadamente, “ ... *SAD computation SHALL be done for each signature operation ...*”

Dado o contexto, relativamente aos limites por “tempo”, estes deverão ser diferenciados consoante o tipo de certificados, designadamente:

- Certificado qualificado de selo eletrónico: Período máximo de 60 dias;
- Certificado qualificado de assinatura eletrónica, que inclua os poderes de representação do titular em relação à entidade, para efeitos exclusivos de faturação eletrónica: Período máximo de 1 dia;
- Restantes certificados qualificados de assinatura eletrónica: É requerida a introdução dos dados de autenticação em cada operação de assinatura.

Os PQSC devem configurar (e criar mecanismos de alerta) os seus sistemas de assinatura/selo eletrónico à distância, de modo a que, de forma periódica, o titular do certificado, necessite introduzir os novos dados de autenticação, de modo a não exceder o período máximo previsto.

Lisboa, 12 de janeiro de 2021

O Diretor-Geral do GNS

António Gameiro Marques
CALM

³ Signature Activation Data

⁴ EN 419241-1:2018: Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements